SmartSuite

Framework / Cybersecurity / Other

CSA IoT Security Controls Framework (IoT SCF) v2

CSA IoT Security Controls Framework v2 (January 2021) is a 21-domain workbook of IoT controls for architects and auditors, now superseded by CSA's IoT Controls Matrix v3.



What it is

The CSA IoT Security Controls Framework version 2 is a workbook of security controls for enterprise Internet of Things systems, released on January 28, 2021 by the Cloud Security Alliance (CSA) IoT Working Group. It has been superseded by the CSA IoT Controls Matrix version 3, published on April 25, 2022, which CSA lists at 198 controls, up from 155 in the first version. This page describes version 2 only.

CSA publishes the framework free of charge, with a companion guide. Aaron Guzman, Michael Roza and Brian Russell led the initiative. The framework is voluntary, has no certification scheme and no regulator behind it. Its stated users are system architects, developers and security engineers designing IoT systems, and auditors and penetration testers who validate controls and their implementations.

At a glance

PUBLISHER Cloud Security Alliance (CSA)	TYPE Standard	VERSION v2 (superseded by the CSA IoT Controls Matrix v3, April 25, 2022)
EFFECTIVE Voluntary; no enforcement date. Version 2 published January 28, 2021	DOMAIN Cybersecurity	FAMILY Other
REGION International (published in the United States)	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY High

Source: cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2

Why it matters

- **Controls sized to impact** Impact levels follow FIPS 199 and FIPS 200. When an impact level is high, all available controls apply, including those for low and moderate levels.
- **Controls assigned to architecture layers** Four columns let users filter for controls that apply to the device, the network that hosts it, a gateway or the cloud service.
- **Implementation guidance in the sheet** Each control is typed as preventive, detective or corrective, marked manual, automatic or semi-automatic, and given a frequency from annually to continuously.
- **A legal domain** Version 2 introduced a Legal domain covering legal assessment, terms and conditions and privacy policy, contracts, disclaimers, notifications, liability and data transfer.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CSA IoT SCF v2

Control Library by Domain

Hold the controls under the 21 domain codes and their control IDs, such as RSM-01, with an owner and review date for each.

Impact Level Tailoring

Record the confidentiality, integrity and availability impact level for each IoT system and show the controls that apply at that level.

Layer Allocation and Residual Risk

Assign each control to the device, network, gateway or cloud layer, and log residual risk and compensating measures where a component cannot comply.

Control Type and Frequency

Capture whether each control is preventive, detective or corrective, manual or automated, and schedule its review at the stated frequency.

Security Testing and Vulnerability Evidence

Attach penetration test, red team and third-party assessment results and vulnerability scan evidence to the controls in the Security Testing and Vulnerability Management domains.

Device Supplier Risk and Reporting

Link device makers and cloud platform suppliers to vendor assessments, and report control status by system and layer.

Common framework mappings

CSA CCM v4

Official resources

CSA IoT Security Controls Framework (Version 2) Specification

Defines the structured guidance for securing IoT systems throughout their lifecycle.

cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2

CSA IoT Security Controls Implementation Guide

Provides an in-depth outline of implementing security controls for IoT deployments.

cloudsecurityalliance.org/artifacts/guide-to-the-internet-of-things-iot-security-controls-framework-v2

CSA IoT Security Controls Framework Version 2 Announcement

CSA press release of January 28, 2021: what changed in version 2 (new Legal and Security Testing domains, consolidated device types), who led it and how controls are allocated.

cloudsecurityalliance.org/press-releases/2021/01/28/cloud-security-alliance-s-new-internet-of-things-iot-security-controls-framework-allows-for-easier-evaluation-implementation-of-security-controls-within-iot-architectures

CSA IoT Controls Matrix v3 (current version)

CSA page for the current IoT Controls Matrix version 3, released April 25, 2022, which supersedes version 2.

cloudsecurityalliance.org/artifacts/iot-security-controls-framework-v3

Frequently asked questions

Is the CSA IoT Security Controls Framework v2 still current?

No. CSA released the IoT Controls Matrix version 3, the renamed successor, on April 25, 2022. CSA's version 3 page lists 198 controls, up from 155 in the first version, and says technical clarity and references improved. Version 2, released on January 28, 2021, remains available on CSA's site.

How are the controls organized in version 2?

The workbook has 21 control domains, such as Asset Management, Secure Communications, Governance, Legal and Security Testing, each with sub-domains. Each control has an ID like RSM-01, a related CSA Cloud Controls Matrix ID in column E and a control specification in column F (Guide to the IoT Security Controls Framework Version 2).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How do I decide which controls apply to my system?

You rate the system's confidentiality, integrity and availability impact as low, moderate or high, using FIPS 199, and filter columns G to I accordingly. If an impact level is high, all available controls apply, including those for low and moderate levels. If it is moderate, the moderate and low controls apply (guide, page 10).

What are the device, network, gateway and cloud columns for?

Columns O to R let you filter controls by the architectural layer that implements them. The framework treats these layers as trust boundaries. Because the allocations are best-case postures, the guide tells the security architect to identify components that cannot comply and plan alternative measures for the residual risk.

Is the framework free, and who maintains it?

CSA's IoT Working Group wrote it and CSA publishes it for free download, with or without an account. The guide carries a copyright notice that limits use to personal, informational and non-commercial purposes, without modification or redistribution. CSA's current release is the IoT Controls Matrix version 3.

License included / downloadable: Yes The Cloud Security Alliance publishes the framework workbook and its guide for free download on its site, with or without an account. The guide carries a CSA copyright notice that allows personal, informational and non-commercial use, without modification or redistribution, and SmartSuite does not include the workbook in the platform.

Full framework page and mappings: smartsuite.com/frameworks/csa-iot-security-controls-framework-iot-scf-v2